10th International Command and Control Research and Technology Symposium

The Future of C2

Command and Control Information Management Strategy (CIMS) provided by an Information Integration Framework

C2 Policy Track

Juan A. Odenwood
Science Applications International Corporation (SAIC)
2231 Crystal Drive, Suite 501
Arlington, VA 22202
(O) 703-328-2011
(F) 703-271-9751
Juan.A.Odenwood@saic.com

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Command and Control Information Management Strategy (CIMS) provided by an Information Integration Framework	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Science Applications International Corporation (SAIC),2231 Crystal Drive Suite 501,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**35**	

ABSTRACT

Access and availability to information is the key to for future command and control with improved access to information as an objective of the DoD's net-centric initiatives. However, net-centric initiatives are being implemented, piecemeal and slowly, through the DoD Data Strategy currently focused at the community of interest level (COI). In order to improve the speed of transformation, take advantage of net-centric concepts, and to manage information for decision-makers, an information management strategy and a information integration framework to implement that strategy is required.

This paper proposes a C2 Information Integration Framework (C2IIF) that provides management of data strategies, value of information, and Communities of Interest (COIs) at the information level and within the context of portfolio oversight. It permits capabilities alignment to meet transformation objectives assures sound management of the Department's IT investment decisions. Through this framework, DoD can improve information sharing with a repeatable, analytical process. Additionally, since legacy applications are included as part of the framework, the strategy provides the means to migrate and evaluate legacy applications and data within the net-centric environment.

Executive Summary

At the highest level of problem definition, the Department of Defense does not sufficiently share information required for operational needs.

- This is especially applicable for current asymmetric threats that require more diverse information to attain situational awareness and develop acceptable courses of action.

- Warfighters in operational situations do not have access to necessary information and do not have access to the capabilities to manage that information.

- The nation's senior leadership does not have visibility of the information necessary to make informed decisions.

- The current acquisition approach with the Services providing inherently joint capabilities still tends to address developing Service needs first and then Joint needs.

- No current overarching integrating concept within CIO's office to actively address information sharing - several contributing and related initiatives are ongoing.

This paper proposes a vision, identifies goals, and describes objectives and examines DOTMLPF solutions. Relationships to ongoing activities and concepts are identified.

A Command and Control Information Management Strategy (CIMS) is proposed as a solution to this problem. The strategy consists of the development of an analytical framework to guide the required assessments and evaluations, a governance process, and a streamlined acquisition process for information integration capabilities.

This paper's scope is limited to the framework with governance and acquisition aspects discussed in other venues. The framework is defined and representative assessments considered with potential follow-on actions.

The paper concludes with recommendations for the path ahead combined with specific actions that implement that path.

Contents

Problem Statement

At the highest level of problem definition, the Department of Defense does not sufficiently share information required for operational needs.

- This is especially applicable for current asymmetric threats that require more diverse information to attain situational awareness and develop acceptable courses of action.
- Warfighters in operational situations do not have access to necessary information and do not have access to the capabilities to manage that information.
- The nation's senior leadership does not have visibility of the information necessary to make informed decisions.
- The current acquisition approach with the Services providing inherently joint capabilities still tends to address developing Service needs first and then Joint needs.
- No current overarching integrating concept within CIO's office to actively address information sharing - several contributing and related initiatives are ongoing.

The following are assertions that expand upon this problem statement.

Operational Needs of Warfighter

Warfighter Current Need

Warfighters in operational situations do not have access to necessary information and do not have access to the capabilities to manage that information – thus the need for 'Power-to-the-edge' concepts.

Current capabilities providing information are focused around organizations with specific locations. Access to these legacy applications requires co-location with a component of the capability-owning organization, resulting in geographically-constrained access.

Warfighters must respond to re-prioritization from national leadership by addressing each year's national leadership guidance and directives for evolving threats. Capability providers must quickly identify gaps and shortfalls in meeting these prioritizations and attain maximum gap fulfillments and shortfall supplements in the shortest time interval.

Warfighter Future Need

The following statement is used as an example of future warfighter need:

"For our forces to effectively use collaborative capabilities and situational awareness, we must enable them to create pictures of the battlespace that are tailored to their needs —User Defined Operating Pictures (UDOPs)—that assemble and present information in a context that is relevant for them….."The UDOP, on the other hand, provides the user the flexibility to select from any available data source, anywhere on the network, those objects that are most useful

to him at any particular time. This also means that any new data source can be utilized almost from the moment it becomes available on the network, rather than requiring a modification to existing systems, as is the case today…. Information integration, horizontally and vertically, to include C2 systems" [1]

Senior Leadership Needs

Current Senior Leadership Need

The nation's senior leadership does not have visibility into the information necessary to make informed decisions. Currently, the senior leadership has to rely upon a piece-part approach with aggregation by different sources using the highest level of information. This approach does not insure common data between the aggregated components was integrated and indeed leaves open the distinct possibility that components derived and presented conclusions based upon conflicting data regarding the same situation.

Future Senior Leadership Need

To adequately respond to the asymmetric threats faced today, the nation's senior leadership needs a national-level information integration approach across all the federal government.

DoD, with a significant portion of the information of interest, needs be funded to initiate an information management strategy (IMS) effort separate from existing weapon's systems. This IMI effort coordinates closely with ongoing and new weapon systems programs and, as possible, leverages existing information capabilities in support thereof.

Acquisition Needs

Current Acquisition Need

The current acquisition approach with the Services providing inherently joint capabilities still tends to address developing Service needs first and then joint needs. The current environment of limited or shrinking budgets exacerbates this problem.

Also, the existing approach to providing information management to promote information sharing is out of date and very cumbersome. It is not focused at providing the information integration necessary for access and availability. Current information management acquisition activities that provide information sharing tend to be, at best, a secondary activity to a larger weapons system program.

Future Acquisition Need

DoD needs the ability to expeditiously acquire information management and integration capabilities that are independent of weapon systems and that are capable of using information associated with any type of weapon system.

Leadership needs the ability to focus resources across the Department towards acquisition of capabilities that provide best value (of information) and 'return on investment'. This requires the ability to dynamically allocate development resources to provide information sharing capability in an expedited manner and be able to match the speed of technology development. This tacitly implies a 'buy' versus 'develop' acquisition approach and in turn requires the DoD to constantly forecast needs to potential industry capability providers.

CIO Needs

Current CIO Need

The following statements describes the situation:

"Today, the CIO is not recognized as the information standard-setting authority for the Department. The Information Age CIO would ensure that Information Age standards and specifications are established for the enterprise." [1]

"Unlike successful firms, DoD lacks an enterprise-wide approach to the management of its ICT resources. Services' authorities, fragmented ICT oversight by various acquisition executives and bureaucratic legacies all impede the development of an integrated approach to information management. " [2]

Future CIO Need

The following statements forecast the future:

"In the Information Age, the Information Age CIO understands that the number one requirement for system engineering is at the strategic and architectural level, without which the CIO will not be able to provide the required, critically-important enterprise-wide management and oversight." [1]

"I suggest the Department leverage the NII charter development to adopt an enterprise-wide approach to information management, in lieu of the fragmented, piecemeal processes we now have." [2]

Summary of Needs

In summary, information access and availability needs are described by the following statement:

"Information integration, horizontally and vertically, to include C2 systems" [1]

This need specification identifies the requirement for more than the ongoing horizontal information integration activities and also the need for vertical information 'compression' activities; i.e. faster provider-to-consumer-to action times.

Problem Analysis

Recognition of need

The needs espoused above have previously been identified and are encapsulated within the following:

> **"Strategy 1.3.1 - *Build a framework to determine the value of information.*** Our military capabilities are heavily dependent on focused information. The value of information is a primary discriminator in business decisions and information assurance protection strategies that focus on priority targets. This strategy requires developing and applying knowledge management methods and tools for helping a customer determine the value of information to their missions and tasks (and the risks of not having the information). This methodology, if successful, can help reduce the "glut" of information and enable DoD to treat information itself as a commodity." [3]
>
> "In this section, the term "information technology architecture", with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals." [4]

This paper proposes that achieving the DoD's 'strategic goals' requires information resource management to

1) Dynamically meet the information sharing needs identified above, and to
2) Rapidly utilize technology advancements that support these strategic goals.

Analysis of Issues

Issues identified in this paper are organized according to the standard DOTMLPF (Doctrine, Organization, Training, Materiel, Leadership, Policy and Facilities). The following is an incomplete representative list of some of the DOTMLPF issues addressed by the CIIMS.

Doctrine

Issue

Operational doctrine now focused on mission description and does not address leveraging information that might be useful in accomplishing mission goals. No existing formalized process exists to identify what information each mission type could utilize and what information each mission type should provide to others. Summary: Lack of information sharing rules, processes, and procedures.

Solution

Full solution:

- Examine each mission type within context of all other mission types that may be related and information shared to and from.
- Determine opportunities for information sharing with these other mission types.
- Categorize and modify/generate the necessary doctrine for each mission type such that information sharing opportunities are exploited to insure maximum mission success as directed by commander's intent.
- Codify this doctrine in the proper documents with rules, processes, and procedures.

Partial

- A partial solution that can be implemented is to first focus only information currently available but not being leveraged by each mission type.

Observation

Doctrine will determine how successful the CIMS is implemented. If the doctrine does not address the full solution then the advantage of CIMS cannot be fully realized.

Organization

Issues

No organization is currently tasked to identify information sharing opportunities across mission types. Current information focus is on specific mission type and occasional opportunistically identified.
There is no current entity that can provide the needed governance oversight and management functions across the diverse set of organizations. Responsibilities, as they exist today, are distributed over multiple diverse organizations.

Solution

Develop a concept of operations for governance
Identify key stakeholders and participants necessary to implement CIMS
Establish the necessary agreements to develop a common governance process with the necessary oversight, management, and support organizational entities.
Initiate the activities of these organizational entities.

Observation

There are core organizations whose participation and agreement are essential to achieving success in applying the CIMS. The most difficult part of initiating the CIMS may well be obtaining the concurrence of these organizations. This will require explaining this strategy in terms that explain how CIMS benefits each organization.

Training

Issues

Employment of this strategy will require usage of modern and reasonably advanced knowledge management and workflow tools not commonly used currently within the DoD.

Employing COIs as currently envisioned also require individuals to have knowledge of other areas traditionally outside of their assigned mission areas.

Solution

In order to maximize advantage of the CIMS, the DoD will need to initiate advanced knowledge management tool training as an integral part of its operational training capabilities.

Cross-mission training will have to be significantly improved and performed other than assigning personnel to various missions. This cross-mission training most likely will require an initial a priori mission area training overview along with refresher courses as missions are added and/or altered.

Observation

The training facilities and access to the necessary knowledge management tools can readily be arranged and operated within the DoD. This may well require new schools to be established along with the definitions of competency and skill levels. The DoD CIO's office should specify standard sets of acceptable knowledge management tools and techniques.

Use of these tools should become an integral part of every operational exercise.

Materiel

Issues

Many opportunities to share information are expected to exist today within the DoD, but are lacking the material solutions required to be provide technologically current accessibility.

Prior to migration into a net-centric environment select legacy applications within existing programs of record will need to wrapped in order to publish and discover information on the Global Information Grid (GIG).

Select legacy applications will be migrated into services within the Net-Centric Enterprise Services (NCES).

New services will be required to publish and discover data onto the GIG. These will replace some legacy applications that are needed but that cannot be migrated and also will provide new capabilities that currently do not exist.

Solution

The CIMS specifically is designed to provide the following solutions through operation of the framework:

Determination of which legacy applications on which to employ wrappers will require analysis of each program of record for it's relative importance, the current state of it's technology, the ability to adequately integrate publishing data and discovery processes onto the GIG into the existing configuration. Other analysis may also be required.

Migration of legacy applications will require assessments of each as to the value of its information, the difficulty and risks of migration and synchronization with other efforts.

Creation of new services that publish and discover data onto to the GIG will need to be prioritized by the governance process

Observation

The set of material solutions, given the massive change from industrial age to information age concepts will be vast.

Much of the required infrastructure is not yet in place with agreements lacking as to what specifically will be provided. Additionally, multiple sets of infrastructures are currently being developed. This unfortunately poses many challenges and obstacles to accomplishing net-centric operations.

The governance process to operate the framework properly is also absent.

Leadership

Issues

Command leadership of C2 activities will need to become aware of how information may be shared to address situations that are not currently within the accepted threat space.

Cultural barriers preventing information sharing will have to be overcome; i.e. that 'information is power' must be discarded.

Leadership must improve on using 'out-of-the-box' thinking and concepts to counter the expected asymmetric threats. Predictability of leadership by the opponent is not desirable in an asymmetric threat environment: it may the element under exploitation.

Solution

Use demonstrations, exercises and training programs to train leadership on how to use information age techniques to improve their mission success against diverse and asymmetric threats.

Stop the cultural drivers to 'hoard' information and redirect these drivers towards information sharing. An example may be to promote on support of joint operations versus support of Service-specific operations.

Actively pursue and recruit individuals who exhibit proficiency at 'out-of-the-box' thinking.

Observation

The increase in the sharing of information will inherently support and improve the success of joint operations. The type of information sharing envisioned from the CIMS supersedes the need for interoperability since the same information is used in multiple places vice the current situation of multiple set of information are used differently in multiple places.

Personnel

Issues

Current personnel may lack the proper background and understanding to achieve proficiency in using information age processes and tools.
Current personnel may need relaxation from over-restrictive doctrinal thinking, i.e. trained to re-think how to solve problems when facing new or existing threats.
(See Leadership and Training)

Solution

Actively pursue and recruit individuals who exhibit proficiency at 'out-of-the-box' thinking

Observation

This may be the most revolutionizing aspect of transformation: transforming to a set of personnel that can fight and use information age concepts to engage in new currently unimaginable combat.

Facilities

Issues

Facilities will need to be dedicated to the training and exercises required by these new information age processes and procedures.
Hosting the required applications and new services onto the GIG may require connections that don't currently exist.

Solution

Select and reserve space within existing facilities or identify new more modern facilities.

Observation

The lifecycle costs of operating these facilities need to be carefully considered when proposing candidate facilities.

Problem Solution

Vision

Access and availability of information is critical for the future evolution of the Department of Defense and especially for the command and control needs of the warfighters. The following statement provides a definition of a vision for the DoD:

> "A vision is a description of a desired end-state. The Department's desired information end-state—its Information Vision—is a ubiquitous, secure, robust, trusted, protected, and routinely used wide-bandwidth network that is populated with the information and information services that our forces need" [1]

Currently much work in the DoD is focused upon providing inter-connectivity. This however does not necessarily lead to interoperability. Interoperability requires that each party understand what the other is communicating, not only that they are communicating something.

No current existing ability within the DoD focuses on integrating information across the myriad of programs of record (PORs) that provide C2 capabilities.

Vision Statement

This paper proposes the following vision statement:

> Assure access and availability to the information wherever and whenever necessary to 1) assure allies, 2) dissuade, 3) deter, and 4) defeat opponents, and 5) defend against attack under any operational environment. This information sharing spans from senior leadership to the warfighter and back and is provided by the Global Information Grid (GIG). The operational environment includes all possible missions for all possible threats and is therefore scenario agnostic, and is also C2 model agnostic.

Goals

To achieve this vision requires an active ongoing effort to insure that information is shared and integrated whenever and wherever needed within the DoD.

> "Many of the capabilities required for agile, distributed operations in the 21st century will be enabled by a global information environment with ubiquitous, assured access to information and situational awareness, when and where any combatant command needs it. The days of "islands" of information – critical information that the warfighter didn't know existed, and that the owner of the information didn't know was important – must be replaced by a global information environment that will provide commanders at all levels access to information regardless of its location –

information that will improve their local situational awareness and the effectiveness of whatever kind of operation the strategic objective requires." [1]

This paper proposes a C2 Information Management Strategy (CIMS) to address the command and control aspects of this problem (with the clear recognition that the approach is extensible to types of information other than C2). The strategy consists of developing and operating an analytical framework to guide the required assessments and evaluations, a governance process to provide the necessary management and oversight, and a streamlined acquisition process for information integration capabilities.

This paper's scope is limited to the framework with governance and acquisition aspects discussed in other venues.

This strategy provides a repeatable methodology, within a mission context, to determine

- What data can be shared,
- What data should be shared,
- Where data needs to be shared,
- If data is being shared, and
- How well data is being shared.

The above constitute the principles upon which the strategy is constructed and operated.

Selected aspects and purposes of the strategy are:

- Identifies data strategy for migration & transition
- Provides strategy to migrate & transition applications into net-centric environment
- Recognizes and leverages large legacy investment in current applications
- Characterizes applications as to need to migrate along with technology
- Determine investment level required to migrate and transition
- Provides means to make decisions on investments to upgrade applications and technology along investments to migrate towards net-centric concept.
-

The strategy must specifically address 'islands of data' concerns by providing a measurable analytical methodology to determine data sharing needs. The framework, as describe below, addresses all of the above topics.

Analytical Framework

To implement the strategy above the DoD needs a framework to guide and provide a basis for information management decisions. The proposed framework uses authenticated information to identify functions performed and also to identify capabilities used by these functions. Substantial risks exists that the current COI focus will result in isolated "islands of information"; the framework is explicitly designed to examine data sharing opportunities across COI areas and feed COI-specific data strategies from a cross-COI

perspective. The framework does not restrict or constrain but enhances and helps identify data management and information sharing needs of the COIs.

Leverage Investment in Legacy Apps

Legacy applications are mapped to the framework to provide the means to migrate and evaluate to net-centric environment. An important piece currently missing in the NII strategy is the ability to leverage authenticated information; e.g., unable to map up-to-date Joint Operational Concepts (JOCs), Joint Integrating Concepts (JICs), Universal Joint Task Lists (UJTLs), and other similar information sources to the applications needed on the GIG. This proposed framework provides the means to leverage this information regardless of the source.

Also lacking today is an overall approach which allows for the expression and evaluation of various policy and technology alternatives for successfully overcoming the issues discussed above. Again, this proposed framework specifically addresses this aspect through the appropriate usage of characterization layers that express and evaluate policies and technologies.

Principles for Information Strategy

The following are proposed principles that are implemented through application of the CIMS. The details of the framework are discussed in subsequent sections.

1. Discover <u>What</u> information can be shared.
This identifies the types of information available to be shared but not whether or not should it be shared. It is contained in the capabilities portion of the framework and is discovered as the strategy is developed.

2. Discover <u>What</u> information should be shared.
This identifies the types of information that should be shared according to existing requirements. It is contained in the Reference Model layer of the framework when it is populated with requirements statements.

3. Discover <u>Where</u> should information sharing occur.
This is identified when the framework is populated with *<u>legacy application and other existing processes</u>*. This is discovered when the strategy is applied to the reference model revealing information sharing opportunities among the needed capabilities. This involves assessments of the needs statements represented in the reference model layer and

4. Discover <u>If</u> information sharing is occurring.
This is identified from an assessment of information sharing opportunities and consists of gaps and shortfalls regarding data sharing. The gaps are identified when the strategy is applied to the portfolio to analyze if information sharing is actually performed every as where needed with the definition of ‘where information sharing needs to occur but doesn’t’. Shortfalls are described below.

5. Discover How well information sharing is occurring.

Assessments of the framework measure information and determine necessary remedial efforts given the expressed prioritizations. These are expressed as shortfalls and are identified when the strategy is applied to the portfolio to analyze information sharing quality and completeness. Specifically, shortfalls occur when information is not shared adequately or as completely required by the reference model's definition

What Framework Provides

Taxonomies

A taxonomy of the C2 functions employed or required by the DoD must be created. This paper proposes that all existing JPUBS, JICS/JOCS, integrating CONOPS, CONOPS and other authenticated source documents be analyzed to identify all required C2 functions. The analysis should focus on a core set of documents and then expand in a manageable manner. The product of this analysis is a taxonomy of all C2 functions required for the DoD. As new functions are identified as a need within the DoD each developing entity is required to examine existing functions to determine leveraging opportunities.

A taxonomy of the C2 capabilities employed or required by the DoD must also be created. Subsequent analysis of each function identifies the individual C2 capabilities required to support these functions. Capabilities are identified and recorded according to a pre-developed specification list with additions as necessary. Consolidating all these function-supporting capabilities to a master list of C2 capabilities creates a taxonomy of all required C2 capabilities. As new functions are initiated and supporting C2 capabilities identified each developing entity is required to examine existing or under-development C2 capabilities in order to exploit leveraging opportunities.

Ontology

An ontology describing the rules of all function and capability interactions must be created. As described later in the paper, evaluation of the intersections between functions and capabilities produces the rules of how each function uses a capability. This serves as the basis for a dynamic C2 ontology that relates the taxonomies of functions and capabilities.

Lexicon

A C2 lexicon is required to provide a common language within the DoD C2 community. The terms identified within the above taxonomies and ontology provides the basis for a C2 lexicon.

Reference Model Layer

A reference model identifying information integration needs is required. The matrix of required capabilities (rows) and the supported functions (columns) provides this basic *reference model* layer of the C2IIF. The intersection point between a function

(column) and capability (row) is indicated positive where a function uses a specific capability, with the default value being negative (unused). Building the reference model layer in this manner captures the definition of functions and their supporting required capabilities much like a requirements definition matrix. That is, if any element is positive then the function (column) uses the capability (row).

To apply limited resources to highest need first, the reference model layer functions are prioritized by the using warfighters, with supporting capabilities being prioritized secondarily. Additions and deletions of reference model functions and capabilities are performed by the appropriate governing entity, providing the means to *manage* required C2 capabilities. Alternative prioritizations are explored from the results produced by assessments of the application and characterization layers.

Applications Layer

The applications layer identifies capabilities from the reference model layer that are supported by existing legacy applications. Mapping all legacy applications to the taxonomy of required C2 capabilities identifies how various functions are supported. This mapping populates intersections in the reference model and reveals non-mapped intersections (gaps) and also multiply-mapped intersections (duplicates). The set of all mapped capabilities provides the basis for a migration portfolio of C2 capabilities that need to be considered for transition to a net-centric compliant form with subsequent publication on the GIG.

The gaps in C2 capabilities identified by the applications layer are coupled with warfighter function prioritizations to create a net-centric new capability portfolio. These gaps are gathered into prioritized groups described in an Initial Capabilities Document (ICD) and used as input into the JCIDS process. Applicable policy and standards are subsequently used to develop these new services, publishing and discovering data as required by the DoD Data Management Strategy.

The migration portfolio of legacy applications and the new capability portfolio combine to provide the means to manage resource allocation in accordance with warfighter prioritization and enables controlled evolution of C2 capabilities in an integrated manner.

This approach explicitly excludes creation of the ‘islands of information’ that exist today. As migration proceeds some legacy applications are wrapped to publish and discover data and are published as services on the GIG. These wrapped legacy applications are evaluated to determine applicability for fulfilling gaps in needed capabilities – non-mapped intersections described above. Other legacy applications are replaced by new services per the new capability portfolio. A percentage of legacy applications are superseded by GIG infrastructure and core enterprise services capabilities and are not expected to undergo migration.

Characterization Layers

As introduced above in the ontology description, detailed evaluation of each intersection of a function with a capability identifies the orchestration of how the capability is used and in turn provides a re-usable orchestration service capability for publication onto the GIG.

When multiple functions use the same capability or similar capabilities, a previously unrecognized opportunity for information sharing possibly exists. Such an opportunity needs further analysis to determine if sharing of information should occur and if and how well it is occurring. This assessment is formalized into a repeatable measurable process and used where applicable. Capability usage by functions is realigned or capabilities consolidated as a result of this assessment, with the sharing (integration) of previously uncorrelated information as a result.

The applications layer is assessed as to implementation characterization (client-server, web-enabled, standalone, etc) with supporting technology, transition/migration plan and schedule and also desired programmatic aspects. From usage identified by analysis of the applications layer, opportunities are identified for consolidations, bundling and related alignment of capabilities.

The business processes associated with one or more capabilities are described within a characterization layer. This affords the opportunity to share and reuse processes as appropriate and also enables business process alignments where desirable and feasible. Coupled with the properly authorized governance and oversight entity, this approach helps prevent re-inventing existing processes ad hoc opportunistically, yet permits controlled evolution.

Multiple characterization layers are used to capture all needed aspects for evaluations required by the information integration framework.

Applied Information Strategy

This section describes the process steps used in applying the strategy to solve the information sharing problem. This process is implemented and operated after the framework reference model layer has been constructed. The following process steps have been identified:

1. Define Selected Program in Terms of Reference Model (C2IIRM)

Analyze the program selected for assessment and develop a definition of the program in terms of the reference model's function-capability pairings. Clearly identify those components that cannot be defined within the context of the reference model.

2. Map Legacy Applications to Appropriate Function-Capability Pairing

Identify legacy application components, described in terns of function-capability pairing, provided by the assessed program and that map to the reference model's pairings. Add these function-capability pairings to the portfolio, clearly identifying their source and status.

3. Map Planned Application Upgrades, New Services to Function-Capability Pairing

Identify applications upgrade components or new services, described in terns of function-capability pairing, provided by the assessed program and that map to the reference

model's pairings. Add these function-capability pairings to the portfolio, clearly identifying their source and status.

4. Identify Unmapped Remaining Legacy Applications

Identify legacy application components, described in terns of function-capability pairing, provided by the assessed program but that don't map to the reference model's pairings. Add these function-capability pairings to the portfolio, clearly identifying their source and status.

5. Identify Unmapped New Services

Identify those new services, described in terns of function-capability pairing, provided by the assessed program but that don't map to the reference model's pairings. Add these function-capability pairings to the portfolio, clearly identifying their source and status.

6. Perform Analysis on Unmapped (4) and (5)

Determine if function-capability pairing exists, if the program's capability needs further decomposition or if it needs to be aggregated with another program's capability in order to map to the reference model's pairings of function-capability. Remap components modified accordingly into the reference model and clearly identify remaining unmapped for use in [2.8].

7. Update Reference Model from Unmapped (6) as appropriate

Add those function-capability pairings that are being performed but are not in reference model. This may involve adding new functions and capabilities to the framework (C2IIF) as well.

8. Resolve Unmapped (1), (5), & (6) Components

Review those components (1), (2) & (6) that cannot be mapped within the context of the reference model. Determine if these are duplicative with respect to infrastructure capabilities or with other related capabilities.

9. Evaluate Reference Model Compliance

Examine assessed program reference-model mapped portfolio entries with respect to their ability to support information sharing across all applicable functions. Compliance must account for each information opportunity that does not support full sharing, those components that duplicate infrastructure capabilities, and those components that do not perform information sharing in concert with net-centric concepts and data management strategy guidance.

10. Develop Deficiency List for Assessed Program

Report all deficiencies identified as gaps in information sharing (missing) that require fulfillment, shortfalls in information sharing (those that do not adequately provide information sharing but do some), and those identified as duplicative with other portfolio entries (for this program and other assessed programs). This deficiency list is then

provided to the applicable governance process for further action and perhaps used as input into acquisition via the JCIDS process.

Framework Provides Ability to Determine?

With the proposed framework sufficiently populated these example questions may then be answered:

- Where is needed data sharing not occurring?
- Is the data sharing occurring sufficiently well?
- Where may be duplication of data?
- What are opportunities to improve data sharing?
- What are opportunities to upgrade technologies?
- Where are opportunities to eliminate and update processes?
- Scope and level of effort required to migrate/transition selected capabilities into net-centric environment?
- What is cost of supplying today's capability in N-C environment?
- What are dependencies of data usage?
- Creator-to-modifiers-to-retrievers…(shows order of migration of applications)
- What is cost estimate for migration/transition? And operation cost in N-C environment? (leads to ROI, trade studies on cost effectiveness of migrations/transitions: i.e. might be better to wait and then rebuild capability as services rather than individually migrate one at a time.)

No Current Capability Can Answer These Questions

Summary

The DoD needs an integrating approach to improve information access and availability across current missions..

Development and management of the layers that comprise the information integration framework (C2IIF), coupled with warfighter prioritization and allocated resources, provide a plan for the transition and migration to net-centric compliant C2 capabilities on the GIG. The C2IIF also plans and manages the prioritized development of new C2 capabilities for publication on the GIG.

The CIMS provides a solution through the C2IIF that guides,– not directs, and is used to propose solutions, not dictums. The strategy helps develop the COIs and does not constrain COIs or other pilot efforts

Identifying previously unrecognized information sharing opportunities between mission functions, when combined with the ability to focus C2 capability evolution, provides an important path towards urgently needed integration of information within the DoD.

References

1. Brown, Bruce K. (LtGen. ,Ret), “Information Strategy”, Unpublished, February 2005.

2. Memo from Admiral Cebrowski, Director of Office of Force Transformation, to Deputy Secretary of Defense, 24 June 2004.

3. Information Strategic Plan, DoDCIO, October, 1999

4. TITLE 40 > CHAPTER 25 > SUBCHAPTER I > Part B > § 1425

Appendix A: Definitions

Information: Any communications or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

Information Management: The planning, budgeting, manipulating, controlling of information throughout its life-cycle (e.g., creation or collection, processing, dissemination, use, storage, and disposition).

Information Resources: Information and related resources, such as personnel, equipment, funds, and information technology.

Information Resources Management: The process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources such as personnel, equipment, funds, and information technology.

Information Services: A discrete set of information activities typically provided on a reimbursable basis. These activities include analysis, acquisition, test, delivery, operation, or management of hardware, software, and communications systems.

Information Superiority: The ability to obtain and transmit information unimpeded to any destination as and when needed and to exploit or deny an adversary's ability to do so. This includes the ability to manage information throughout its life-cycle, i.e., to create, collect, process, disseminate, use, store and dispose of an unimpeded flow of information while exploiting or denying an adversary's ability to do the same.

Information Technology: (A) Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

(B) The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

(C) Notwithstanding subparagraphs (A) and (B), the term 'information technology' does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Infrastructure: Infrastructure is used with different contextual meanings. Infrastructure most generally relates to and has a hardware orientation but note that it is frequently more comprehensive and includes software and communications. Collectively, the structure must meet the performance requirements of and capacity for data and application requirements. Again note that just citing standards for designing an architecture or infrastructure does not include functional and mission area requirements for performance. Performance requirement metrics must be an inherent part of an overall infrastructure to provide performance interoperability and compatibility. It identifies the top-level design of communications, processing, and operating system software. It describes the performance characteristics needed to meet database and application requirements. It provides a geographic distribution of components to locations. The infrastructure architecture is defined by the service provider for these capabilities. It includes processors, operating systems, service software, and standards profiles that include network diagrams showing communication links with bandwidth, processor locations, and capacities to include hardware builds versus schedule and costs.

Applications Framework Process;

The migration of DoD C2 Programs and Initiatives to a Net-Centric Capability-based Environment

Juan Odenwood

June 2005

Problem Statement

- Point-to-Point architecture with current analysis processes coupled with management of programmatic milestones will not allow DoD to achieve transformation
- The DoD requires an information environment that allows for:
  - Agile, robust, interoperable and collaborative
  - Sharing of knowledge between war-fighter, business, and intelligence users
  - Combined capabilities from multiple services to form new capabilities
  - Process for programs to be “Born Joint”
- Must leverage very significant investment in legacy applications

DoD requires approach to Migrate & Transition Legacy Applications to Net-Centric Capabilities

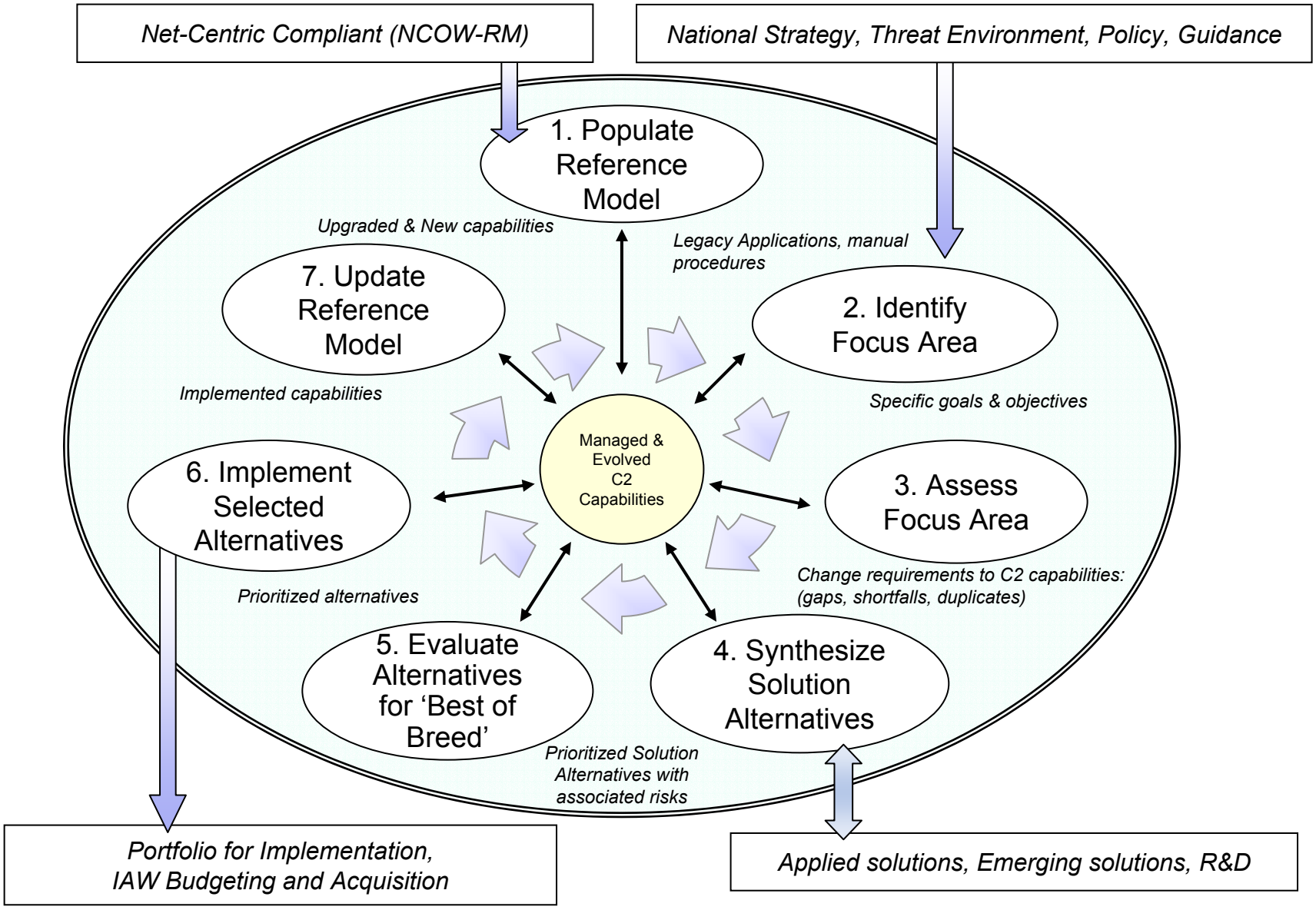
Goal

- Process to evolve from current Point-to-Point DoD IT inventory to utilization of NCES infrastructure
  - Establish model to populate GIG with services for:
    - Increased information sharing
    - Improved decision-making activities
    - Improved self-synchronization of participants
  - Map to existing business aspects of Department in systematic manner
    - KPP, Requirements, UJTL's
  - Combine capabilities from multiple services to form new capabilities and value-added services
    - Combine and tailor services on demand to meet mission requirements.
  - Leverage legacy application investment
    - Migrate Legacy Applications to Net-Centric Services

Flexible Speed of Command for the Warfighter

Migrate Legacy Applications to Net-Centric Services

Application Framework Process



1. Populate Reference Model

- Perform requisite Functional Analysis to determine Departmental C2 functional needs
  - Construct C2 business model for Department
- Identify inclusive and exhaustive set of C2 capabilities required to meet functional needs
  - Ongoing continuous process of discovery and update
- Identify ***HOW*** these needs are currently met
  - Is each need actually met?
  - Is need met with a legacy application?
  - Is need addressed within Planned or Development activity?
- Extend existing NCOW Reference Model to represent this information

2. Identify Focus Area

- Identify area of focus within extended Reference Model
- Prioritization of focus is based upon
  - National Strategy,
  - Threat Environment,
  - Policy,
  - Guidance
- Identify functions employed within this ‘Focus Area’
  - As identified within Reference Model
- Identify supporting capabilities required by these functions
- Identify specific goals and measurable objectives that focus area must achieve
  - Bound focus area for subsequent assessment
  - Establish evaluation criteria

3. Assess Focus Area

- Establish appropriate scenarios and use cases required to assess focus area
  - Reused as possible; made available for subsequent reuse
- Construct focus area within assessment environment
- Insure that assessment generates necessary information according to evaluation criteria
- Execute assessment and collect measurement results
- Analyze results with respect to established goals and objectives
  - Identify potential capability gaps, shortfalls, and duplication

4. Synthesize Solution Alternatives

- Collect gaps, shortfalls, and duplicates
- Identify potential solution alternatives from
  - Applied & existing solutions,
  - Emerging & under development solutions,
  - R&D
- Identify risks associated with each solution alternative
- Rank solutions by risks
- Develop recommended prioritizations of alternatives
- Group solutions alternatives
  - Insure consistent technical approaches within a group
  - Results in sets of solution alternatives fro subsequent evaluation
  - Alternatives can be members of multiple groups

5. Evaluate Alternatives for 'Best of Breed'

- Determine which group of solution alternatives are best choice to implement
  - Measure against scenarios and use cases developed in Focus Area assessment
- Decisions include Budgeting and Acquisition
- Consideration must include
  - If migration of capability necessary?
  - Is replacement under development elsewhere?
  - Can legacy ability be maintained in meantime?
- Solution Alternatives grouped into prospective portfolio
  - Rank ordered as to best meeting goals and objectives established for originating focus area assessment

6. Implement Selected Alternatives

- Identify selected Solution Alternative Portfolio that ‘best’ meets goals and objectives
- Develop risk mitigation approach
- Measure implementation of portfolio for contribution to objectives
  - Cost
  - Schedule
  - Technical performance
- Adjust portfolio elements as required to maintain
  - Baseline costs, schedules, risks, and performance
- Collect technical and programmatic decisions
  - For subsequent process improvement

7. Update Reference Model

- Update extended NCOW Reference Model with
  - Function additions, upgrades and removals
  - Capability additions, upgrades and removals
  - Technical and programmatic decisions
- Include information from
  - Completed portfolio implementation
  - Under development as reflected in element baseline information
- Prepare for identification of next ‘Focus Area’

Summary

- Applications Framework is a path to achieve migration to net-centric capabilities
- Requires commitment and awareness from DOD at level of Y2K
  - But ongoing Transformation already does!
- Successful execution depends upon governance and oversight integrated with ongoing budget and acquisition processes